STATE OF VERMONT
Agency of Administration

STANDARD STC State Technology Collaborative	ORIGINAL POLICY ADOPTED BY STC DATE: 06/10/96	ORIGINAL POLICY NUMBER 01-01-04
	EFFECTIVE DATE	ASSOCIATED DOCUMENTS 0501.012005 Passwords

STATUTORY REFERENCE OR OTHER AUTHORITY:
1 V.S.A. 316(d)
1 V.S.A. 317 (b)
3 V.S.A. 218 (a)
Personnel Policies and Procedures
ELECTRONIC COMMUNICATIONS AND INTERNET USE -
http://www.state.vt.us/pers/er/pm/pm117.htm

APPROVAL DATE:

APPROVED BY: **Secretary of Administration**

STANDARD TITLE: **Passwords**

STANDARD STATEMENT: **The State of Vermont information assets shall be protected from inappropriate access. The proper use of a password represents the best first step in protecting those assets. The password policy and standard makes everyone aware of what they should be doing. At the same time, it is well understood that implementing a standard across an enterprise is difficult. Exception procedures, giving discretionary control to the CIO, are incorporated into the policy.**

Apart from the actual standards, general guidelines and best practices are provided to assist in the optimal use of passwords. Password implementation schemes in commercial products may not meet all the guidelines and best practices. Judgment, based on the value of the assets being protected, will need to be applied when implementing passwords. Password construction and use shall conform to the standards set forth in this policy.

1. General Standards

A. All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on at least a monthly basis. The minimum interval can be extended if advanced methods are used to restrict and track root level access (e.g. sudo, secureID)
B. All user-level passwords (e.g., email, web, desktop computer, etc.) must be routinely changed. The recommended change interval is every two months and must not exceed four months.

C. The change interval can be extended to 1 year if all of the standards are met, and the use of “strong” passwords as defined in the guidelines are required and enforced by a department.
D. Any user account that goes unused for a period of two months will be disabled. For unusual circumstances, exceptions are allowed if fully documented.
E. Distribution of passwords must not be inserted into clear text email messages or other forms of clear text electronic communication. A secure method of distribution must be used. I.e.; PGP, PKI, other encryption
F. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
G. All user-level and system-level passwords should make every effort to conform to the guidelines described below

2. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

A. must support authentication of individual users, not groups.
B. must not store passwords in clear text or in any easily reversible form.
C. must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
D. must support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
E. Applications should support delegation to eliminate the need to share passwords.

3. Use of Passwords and Passphrases for Remote Access Users

Access to the Agency\Department Networks via remote access is to be controlled using either GOVnet TACACS+ authentication, VPN’s or a public/private key system with a strong passphrase.

4. Passphrases

All of the rules above that apply to passwords apply to passphrases.

5. Best Practices

Do not use the same password for Agency\Department accounts as for other non-Agency\Department access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Agency\Department access needs. For example, select one password for the application systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share Agency\Department passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Here is a list of “Do’s”:

A. Do make sure your password is secure
B. Do respect other’s passwords (turn your head when they are entering them, etc.)
C. Do encrypt your passwords if you require storing them.
D. Do change your password when ever it has been shared or compromised
E. Do change your passwords every two months
F. Do configure your workstation to be password protected when your screen saver pops on
G. Do make sure your screen saver is set to come on after 15 minutes of being unattended
H. Do get a phone number from anyone asking for password information
I. Do report any violation of password configuration to the appropriate personnel

Here is a list of "Don’ts":

A. Don't reveal an admin / system password over the phone to ANYONE
B. Don't reveal a password in an email message
C. Don't reveal a password to your supervisor
D. Don't talk about a password in front of others
E. Don't hint at the format of a password (e.g., "my family name")
F. Don't reveal a password on questionnaires or security forms
G. Don't share a password with family members
H. Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Vermont CSIRT.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger, Internet Explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change user level passwords at least once every four months (except system-level passwords which must be changed monthly except departments complying with item C in the general standards) The recommended change interval is every two months.

If an account or password is suspected to have been compromised, report the incident to Vermont CSIRT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Vermont CSIRT (Computer Security Incident Response Team) or its delegates with prior written notice given to the systems manager, department manager or commissioner responsible for the system being audited. Written notice will include:

- Scope of password audit including specifically what systems' accounts (servers, switches, PCs, etc.) are to be tested, dates of testing, stopping points, from what locations and listing methodology and tools.
- Definition of Roles and Responsibilities including names of individual test team members and their monitors, Auditors, System Owners (CIO and functional area managers), System Administrators and Contractors (if applicable).
- Clear, complete, exact statements on distribution of results of testing including viewing of monitors during testing, handling of all reports, logs and testing output, defined destruction method and date of all output by CSIRT and delegates and report of results to department being audited.
- Statement of reports to be given to the systems manager, department manager or commissioner being notified of audit.
- Written verification by the systems manager, department manager or commissioner receiving the written notice that either
    - confidentiality/non-disclosure of information agreements are not required by the department being audited or
    - confidentiality/non-disclosure agreements defined by and required by the department being audited have been signed and dated by all individuals (including individual contractors) performing and monitoring the testing and are on file with the department being audited. This non-disclosure agreement may include requisite training as defined by the department being audited. Such training as required will be specified in the agreement.

If a password is guessed or cracked during one of these scans, the manager, department manager or commissioner responsible for the system will be notified that corrective actions are required.

6. General Password Construction Guidelines

Passwords are used for various purposes at the Agency\Departments within the State of Vermont. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

A. The password contains less than eight characters
B. The password is a word found in a dictionary (English or foreign)
C. The password is a common usage word such as:
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, software.
    c. Birthdays and other personal information such as addresses and phone numbers.
    d. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    e. Any of the above spelled backwards.
    f. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

A. Are adequately complex in that they are made up of a combination of at least three of the 4 following characteristics;
    1. Contain lower case characters (e.g., a-z),
    2. Contain upper case characters (e.g., A-Z),
    3. Contain digits (e.g. 0-9),
    4. Contain punctuation / special characters (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
B. Are at least eight alphanumeric characters long.
C. Are not a word in any language, slang, dialect, jargon, etc.
D. Are not based on personal information, names of family, etc.
E. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

    NOTE: Do not use either of these examples as passwords!